AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method for utilizing a public wireless local area network (WPAN) for a client with a smart card, comprising:

creating a one-time entropy generated ~~session~~ password for a client based on an identification information of the client, an encryption key provided by the WPAN, and a predetermined text character string;

storing the one-time entropy generated ~~session~~ password and identification information of the client on a public wireless local area network; and

utilizing the one-time entropy generated ~~session~~ password and identity information of the client to authenticate the client in the public wireless local area network.

2. (Original) The method of claim 1 wherein the authentication is provided by a Remote Authentication Dial-In User Service (RADIUS) server.

3. (Previously Presented) The method of claim 1 further comprising authenticating the client by a server associated with said WPAN based on a smart card.

4. (Previously Presented) The method of claim 1 further comprising authenticating the client by a server associated with said WPAN based on a universal subscriber identity module card.

5. (Previously Presented) The method of claim 1 further comprising authenticating the client by a server associated with said WPAN based on a subscriber identity module card.

6. (Original) The method of claim 1 further comprising modifying accounting data from the public wireless local area network to include charging data record fields for the client.

7. (Original) The method of claim 1 wherein the creating is independently performed by each of two entities.

8. (Original) The method of claim 1 wherein the creating comprises utilizing international mobile subscriber identity (IMSI) of the client.

9. (Original) The method of claim 1 wherein the creating comprises utilizing a pseudonym of the client.

10. (Previously presented) The method of claim 1 wherein the creating comprises utilizing Point-to-Point Encryption Send-Key.

11. (Previously presented) The method of claim 1 wherein the creating comprises utilizing Point-to-Point Encryption Recv-Key.

12. (Currently amended) The method of claim 1 wherein the creating comprises: calculating a hash value comprising a plurality of octet values; and converting each of the plurality of octet values into an alphanumeric octet value.

13. (Currently amended) The method of claim 1 wherein the creating comprises; calculating a hash value using a SHA-l hashing process, the hash value comprising a plurality of octet values; and converting each of the plurality of octet values into an alphanumeric octet value.

14. (Currently amended) A system for utilizing a public wireless local area network for a client with a smart card, comprising:

a smart card for a client; and

a first adapter for generating a one-time use ~~session~~ password for the client, based on an identification information of the client, an encryption key provided by the WPAN, and a text character string, wherein the password is used for authenticating the client by a Remote Authentication Dial-In User Service (RADIUS) server.

15. (Original) The system of claim 14 further comprising a second adapter for authenticating the client by a second server based on the smart card.

16. (Previously Presented) The system of claim 15 wherein the first and second adapters reside on separate devices.

17. (Original) The system of claim 15 further comprising a third adapter for modifying RADIUS based accounting data to generate General Packed Radio Server (GPRS) based accounting data.

18. (Previously Presented) The system of claim 17 further comprising a fourth adapter for generating the password for the client.

19. (Currently amended) A method for adapting a public wireless local area network for a client with a smart card, comprising:

creating a one-time use ~~session~~ password for a client based on an identification information of the client, an encryption key provided by the WPAN, and a text character string;

storing the password and the identification information on a Remote Authentication Dial-In User Service (RADIUS) server;

utilizing the password and the identification information to authenticate the client on the RADIUS server; and

modifying RADIUS based accounting data to generate General Packed Radio Server (GPRS) based accounting data for the client.

20. (Currently amended) The method of claim 19 wherein:

the creating comprises deriving the ~~following:~~ password [[=F]] ~~(generating~~ from a hash value ~~(Username.vertline.n*Value-.vertline."sim direct")), wherein Username comprises~~ based on the identification information of the client, the encryption key provided by the WPAN, and the text character string, the hash value comprising a plurality of octet values; and

converting each of the plurality of octet values into an alphanumeric octet value,

wherein ~~Value~~ the encryption key provided by the WPAN is selected from the group consisting of: Kc, which is a 64 bit ciphering key known in the art; Point-to-Point Encryption Send-Key; and Point-to-Point Encryption Recv-Key~~, wherein F is a function for converting a hash value into an alpha-numeric string~~.